

DDRS

Data Management Security

Table of Contents

DDRS Data Management Security	3
1.0 DART Product Security	3
1.1 Creating a User Record	5
1.2 Changing an Existing User Record	6
1.3 Deleting an Existing User Record	6
2.0 DART Web Product Security	7
2.1 Creating a User Record	8
2.2 Editing an Existing User	9
3.0 CORM System Security	11
4.0 BQIS/DA Web-Based Incident Reporting System Security	12
5.0 DDRS Web-Based Tools Security	13

DDRS Data Management Security

The DDRS Data Management team provides support for the following products:

- DART
- DART Web
- CORM
- BQIS/DA Web-Based Incident Reporting
- DDRS Web-Based Tools website

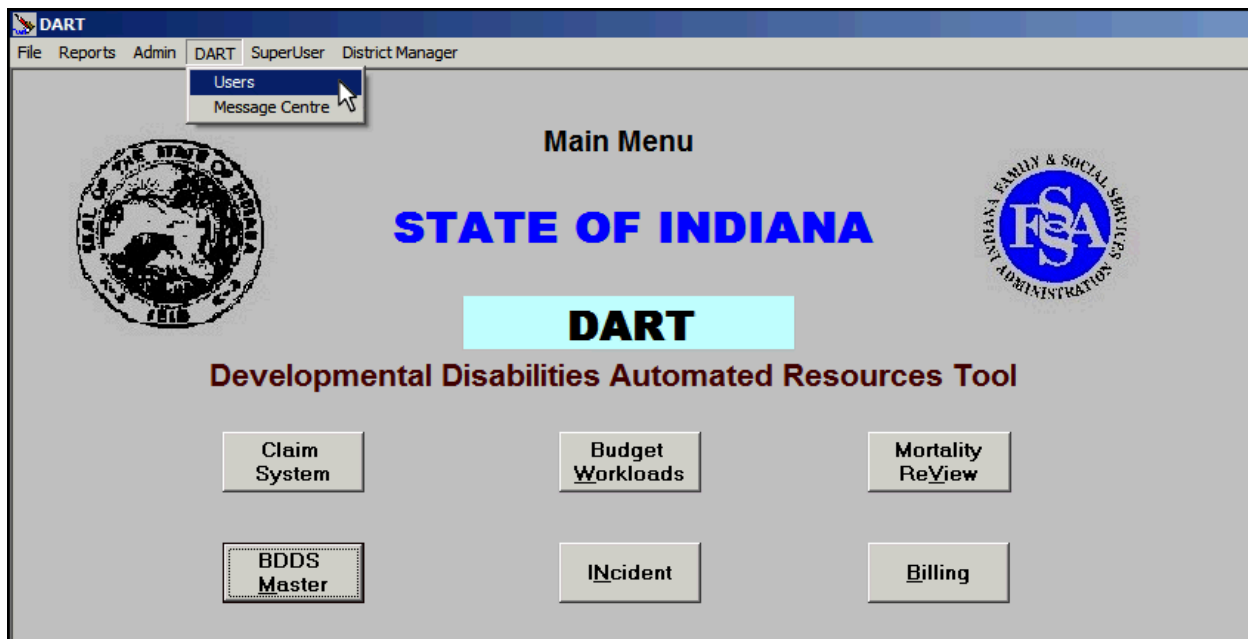
This document describes the security measures that these products use.

See Also

For more information about the standard user functionality of one or more of these products, refer to the product user guides.

1.0 DART Product Security

The Developmental Disabilities Automated Resource Tool (DART) product uses the **User Listing** window to control security for each user. To display the **User Listing** window, select **Users** from the **DART** menu, as shown in the following illustration.



The following illustration shows an example of the **User Listing** window.

User Listing

Users						
	Name	User Name	Password	Flags	Profile	E-mail
	Encinias, Raymond A	RAE1	*****	d	DARTUser2	rencinias@fake.in.gov
	Enker, Larisa M	lenker	*****	d	DUser1	lenkerm@fake.in.gov
	Engott, Daniel R	dengott	*****	d	DARTUser2	dengott@fake.in.gov
	Falkenburg, Andrew R	arfalkenburg	*****	iahcm	Smith1	andy.falkenburg@fake.state.in.c
	Fancher, Angela L	lafancher	*****	12achmr	DartUser27	angie.fancher@fake.in.gov
▶	Farra, Kent M	farrakm	*****	alir	FarraKM	kent.farra@fake.in.gov
	Feagans, Britt	feagansb	*****	4acho	Smith1	feagansb@fake.state.in.gov
	Felter, George S	gsfelter	*****	d	GSFelter	george.felter@fake.in.gov
	Ferguson, Cheryl D	fergiecd	*****	abc3	FergusonCD	cheryl.ferguson@fake.state.in.q
	Fess, Stephen R	fesssr	*****	nop1	SRFess	stephen.fess@fake.in.gov
	Finch, Sidd S	finchss	*****	am	Sfinch	sidd.finch@sjoke.in.gov
	Fiore, Allen D	adfiore	*****	234s	FioreAD	allen.fiore@fake.state.in.gov
	Firenze, Brena M	FirenzeBM	*****	irf13	Smith2	brena.firenze@fake.in.gov

Full Name: Farra, Kent **HIPAA compliant:** ☒ **YES** **Date:** 05/24/2007
Display Name: Kent Farra
Title: Tech Writer **BDDS Staff:** (* Staff is NOT active)
User Name: FarraKM
Password: *****
Flags: iahcm1fs (no commas)
IR Security:
Division: D
Profile: FarraKM
E-Mail: kent.farra@fake.in.gov

Flags Legend:

- NONE - User Rights
- 0(Zero) - Claim System Data Entry Rights
- 1 - Fiscal SC Data Entry Rights
- 2 - Fiscal DM Data Entry Rights
- 3 - 317 Code Rights
- 4 - MRC - Full Rights
- 5 - MRC - Analyst Rights
- 6 - MRC - Read-only
- 9 - Deceased Incident E-Mail
- a - Administrator Rights
- b - Billing Rights

You can use the **User Listing** window to:

- Create a user record.
- Change an existing user record.
- Delete an existing user record.

Important

You must possess Administrator rights to create a new user record, or to change or delete an existing user record. If you are a new user, contact your Systems Administrator to create your user account.

1.1 Creating a User Record

Use the following procedure to create a new user record.

1. Select the **New** button at the bottom of the **User Listing** window. The system adds a new row to the user grid and moves the cursor to the **Full Name** field.
2. Complete the information in the **User Listing** window.

Tip

The **Flags Legend** list box in the **User Listing** window contains the following valid entries for the **Flags** field. You can enter one or more values with no spaces or commas.

NONE - User Rights
0(Zero) - Claim System Data Entry Rights
1 - Fiscal SC Data Entry Rights
2 - Fiscal DM Data Entry Rights
3 - 317 Code Rights
4 - MRC - Full Rights
5 - MRC - Analyst Rights
6 - MRC - Read-only
9 - Deceased Incident E-Mail
a - Administrator Rights
b - Billing Rights
c - Incident Delete Rights
d - Display only Rights
e - Extra Editing Rights
f - Fiscal Access Rights, BFS Verification Data Entry rights
h - Incident Priority High(Closed, Review) Rights
i - Incident Access Rights
k - Provider rights
l - SGL/LP Provider rights
m - User Maintenance rights
n - EDS User Rights
o - OMPP User Rights
p - Waiver Specialist Targeting Rights
r - Only Displaying Incident Rights
s - Super User - Administrator rights, Data Maintenance
t - Fiscal Exception Review Team Data Entry Rights
u - Delete Fiscal rights, OverWriting Fiscal/Billing Rights
w - OverWriting Billing Rights
y - Fiscal BDDS Director Data Entry Rights
z - Fiscal Import Data Rights

-
3. Select **Save**.

1.2 Changing an Existing User Record

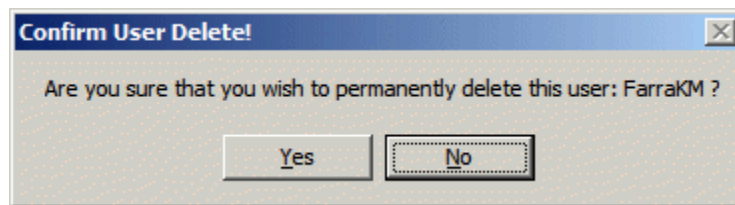
Use the following procedure to change an existing user record.

1. Select the record to change from the user grid.
2. Select the field to change on the user record and delete or change the information.
3. Repeat Step 2 as necessary to change additional information.
4. Select **Save**.

1.3 Deleting an Existing User Record

Use the following procedure to delete an existing user record.

1. Select the record to delete from the user grid.
2. Select **Delete**.
3. Select **Yes** in the **Confirm User Delete** window. The following illustration shows an example of the **Confirm User Delete** window.



2.0 DART Web Product Security

The DART Web product uses the following windows to control security for each user:

- **Add a User** window to create a user record
- **Edit a User** window to edit an existing user record

You can access these windows by using the **Admin** menu in the **WEB INCIDENT EXAMINATION APPLICATION – NEW BDDS INCIDENTS** window, as shown in the following illustration.

WEB INCIDENT EXAMINATION APPLICATION - NEW BDDS INCIDENTS

File View **Admin** Help

INCIDENT: 06/13/2007 Incident Time: 02:20 PM

Where: [Dropdown] Other: [Text Box]

IS FOLLOW-UP REQUIRED? [Dropdown] **RESPONSIBLE FOR FOLLOW-UP** [Dropdown] Date Received: 06/14/2007

Action Completed Date: [Text Box] ☐ Non-Reportable Report?

☐ Is this incident regarding the DEATH of this consumer?
☐ Is this incident regarding a PRN that was administered to this consumer?

CUSTOMER RECORD 1 OF 1

SSN: 123-45-6789 FIRST NAME: TIMOTHY LAST NAME: ALLEN

DOB: 09/25/1956 GENDER: MALE PRIMARY FUNDING SOURCE: SGL

ADDRESS: 1855 WESTWOOD DRIVE COUNTY: POSEY

CITY: MT. VERNON STATE: IN ZIP CODE: 47620

Customer Navigation: [Left Arrow] [Right Arrow]

DART Incident #: [Text Box] Incident Record 1 of 46 [Previous] [Next] [First] [Last]

Change View

NEW

E-Mail Sent [Text Box]

Find [Text Box]

Export to Dart!

Delete Report

Customers

Informed

Reporting Info

Narratives

Occurrences

DART Incidents

EXit

Important

You must possess Administrator rights to create a new user record or to edit an existing user record. If you are a new user, contact your Systems Administrator to create your user account.

2.1 Creating a User Record

Use the following procedure to create a new user record.

1. Select **Add A User** from the **Admin** menu. The **Add A User** window appears.

The screenshot shows a web-based form titled "Add A User". The form is organized into several sections. At the top left, there are fields for "LOGIN ID" and "PASSWORD". To the right of these fields are three buttons: "Save", "Clear", and "Close". Below the "PASSWORD" field is a "DIVISION" dropdown menu. Further down are single-line text input fields for "LAST NAME, FIRST NAME", "SMTP SERVER", "E-MAIL ADDRESS", "TITLE", and "BUREAU". At the bottom, there is a "SECURITY FLAGS" field with a text box and a label that reads "Flags: 'A' = Administrator" in red text.

2. Complete the information in the **Add A User** window.

Tip

Valid entries for the **Security Flags** field include:

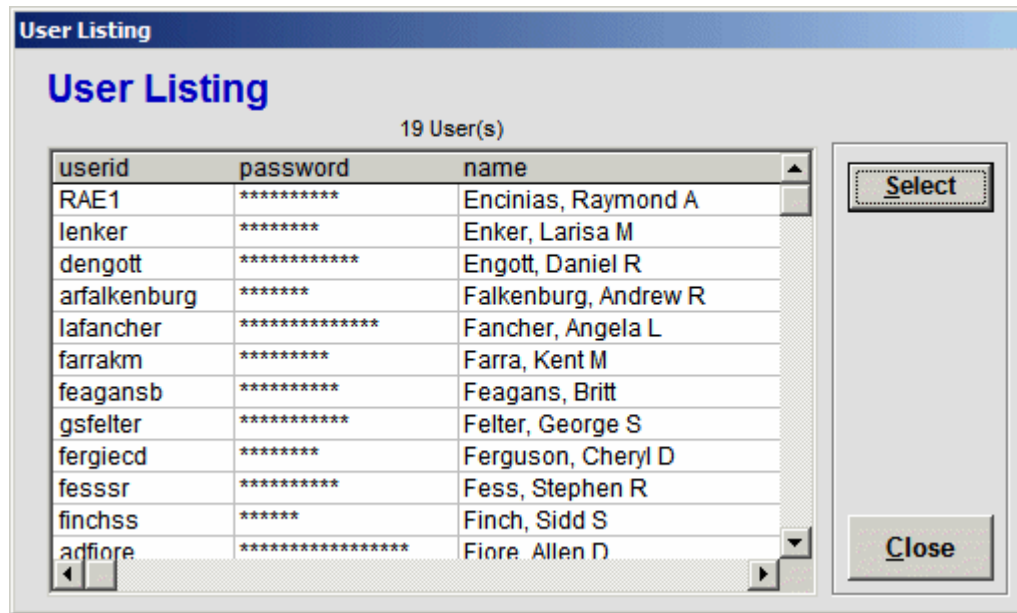
- A for administrator
- D for delete

3. Select **Save**.

2.2 Editing an Existing User

Use the following procedure to edit an existing user record.

1. Select **Edit Users** from the **Admin** menu. The **User Listing** window appears.



2. Select the user to edit from the user grid and click **Select**. The **Edit A User** window appears.

The following illustration shows an example of the **Edit A User** window.

The 'Edit A User' window displays the following information and controls:

- Last Login:** 7/11/2007 9:30:00 AM
- Last Logout:** 7/11/2007 8:45:00 AM
- LOGIN ID:** FARRAKM
- PASSWORD:** PASSWORD
- DIVISION:** D (dropdown menu)
- LAST NAME, FIRST NAME:** KENT FARRA
- SMTP SERVER:** FSS00EX2
- E-MAIL ADDRESS:** KENT.FARRA@FSSA.IN.GOV
- TITLE:** TECH WRITER
- BUREAU:** BDDS
- SECURITY FLAGS:** A
- Flags:** "A" = Administrator
- Buttons:** Edit, Save, Cancel, Close

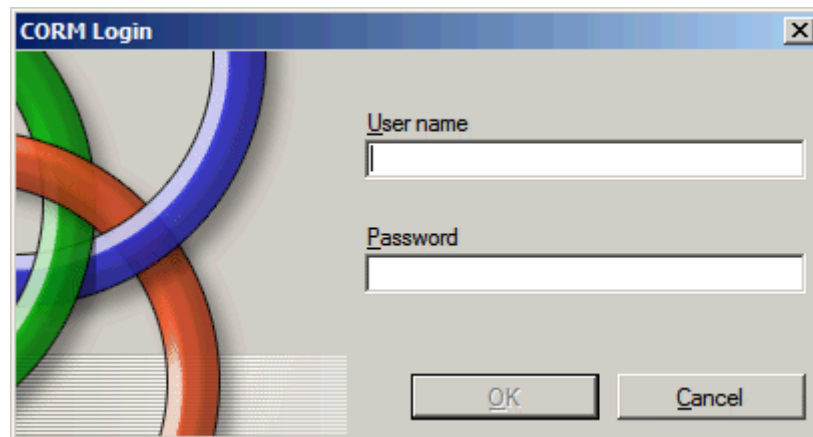
3. Select **Edit** and complete the information in the **Edit A User** window.
4. Select **Save**.

3.0 CORM System Security

During the login process, the CORM product evaluates your user role to determine your access level. If your user role is limited to either Crisis or Outreach, the system modifies the appropriate windows, tabs, and menus. Additionally, capability limitations exist for each role. The CORM product uses the following roles:

- Read-Only
- Crisis Operator
- Outreach Operator
- Crisis Manager
- Outreach Manager
- Crisis Director
- Outreach Director
- Administrator

The following illustration shows an example of the **CORM Login** window.



See Also

For more information about the CORM system, refer to the *CORM System User Guide* in the CORM document library on the DDRS website at:

<https://myshare.in.gov/fssa/ddrs/default.aspx>

4.0 BQIS/DA Web-Based Incident Reporting System Security

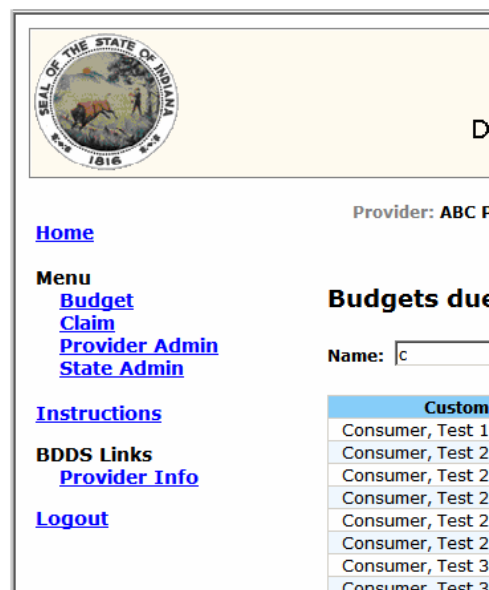
As with many web-based applications, the Incident Reporting System is an open system that permits access to all users. Open systems typically rely on an anonymous user account to control the level of access for users. While a website developer or IT manager could manipulate the anonymous user account to apply security measures to specific parts of the site, this has not occurred in the Incident Reporting System and any user can access all areas of the website.

5.0 DDRS Web-Based Tools Security

During the login process to the DDRS Web-Based Tools website, the system evaluates your user role to determine your access level. The system can limit your user role to one or more of the following tasks that appear as links in the menu structure on the left side of the screen:

- Process a budget
- Process a claim
- Provider administration
- State administration

The following illustration shows an example of the DDRS Web-Based Tools menu structure. (Most users will only see the **Budget** menu, the **Claim** menu, or both.)



If this is the first time that you have logged in to the site, you must set the website as a Trusted Site in your Internet browser. The following message appears.

WARNING! A budget will not be able to be previewed until the following is completed.

In order for this website to function properly, you must add this website as a 'Trusted Site' in your Internet Explorer browser. Please complete the following steps:

1. Click on 'Tools' in the main menu bar
2. Click on 'Internet Options...' in the pull-down list
3. Click on the 'Security' tab of the 'Internet Options' window
4. Click on the 'Trusted Sites' icon
5. Click on the 'Sites...' button
6. Make sure the box for 'Require server verification (https:) for all sites in this zone' is NOT checked
7. In the 'Add this Web site to the zone:' textbox, type 'ddrsprovider.fssa.in.gov'
8. Click the 'Add' button; The website name will now appear in the 'Web sites:' box
9. Click the 'OK' button on each of the two windows that are open
10. Click on the refresh icon in Internet Explorer or press the 'F5' key on your keyboard to refresh the web page
11. Click on the 'Return Home' link below these instructions; This will take you to the website Home page where you will need to click the 'Login' link again to go to the Login page

For further information, you can go to the following Microsoft website:

<http://www.microsoft.com/windows/ie/ie6/using/howto/security/settings.msp>

[Return Home](#)

Follow the instructions to properly set your computer to be able to view and use the website.
When you complete the instructions, the **Log In** window appears.

Log In

User Name:

Password:

Log In

If you do not remember you username and/or password, please contact your provider representative. The Bureau of Developmental Disabilities Services does not retain individual usernames or passwords for this budget tool.

Notice

We are gathering user IP addresses to help in the prosecution of unauthorized use of this website. If you are not an authorized user of this website you should exit now.

Complete the information in the **Log In** window and select **Log In** to access the website.

See Also

For more information about the DDRS Web-Based Tools website, refer to the *DDRS Web-Based Budget Tool User Guide* in the BDDS document library on the DDRS website at:

<https://myshare.in.gov/fssa/ddrs/default.aspx>
